(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 294 248 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **88400930.9**

(22) Date de dépôt: **15.04.88**

(51) Int. Cl.[4]: **G 07 F 7/10**
H 04 L 9/00

(30) Priorité: **20.05.87 FR 8707093**

(43) Date de publication de la demande:
07.12.88 Bulletin 88/49

(84) Etats contractants désignés:
BE CH DE ES GB GR IT LI LU NL SE

(71) Demandeur: **ELECTRONIQUE SERGE DASSAULT**
55, quai Marcel Dassault
F-92214 Saint-Cloud (FR)

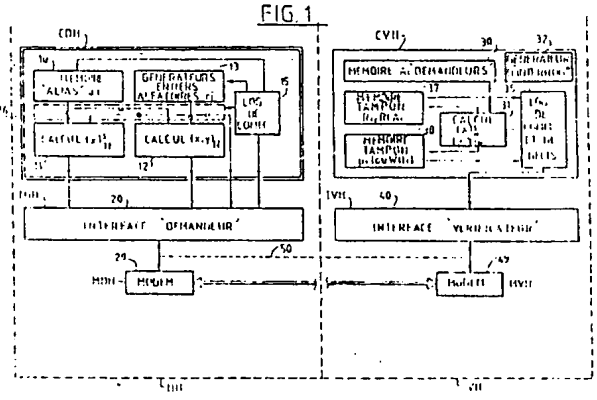
(72) Inventeur: **Collin, Thierry**
88, rue Sylvestre
F-92400 Courbevoie (FR)

(74) Mandataire: **Plaçais, Jean-Yves et al**
Cabinet Netter 40, rue Vignon
F-75009 Paris (FR)

(54) Dispositif et procédé d'habilitation informatique ou télématique.

(57) Un poste demandeur d'habilitation (DH) comprend dans un circuit protégé (CDH) une mémoire bis de données d'habilitation ou alias (a_i) ainsi qu'un générateur (13) d'entiers aléatoires (r_i) et des moyens de calcul (11 et 12) propres à effectuer respectivement une opération d'élévation à une puissance entière modulo N et une multiplication modulo N, N étant par exemple un nombre premier. Ne sortent du circuit secret (CDH) qu'une première quantité représentant le transformé d'un entier aléatoire (r_i) par la première opération ou une seconde quantité représentant soit cet entier aléatoire lui-même, soit le produit de cet entier aléatoire par l'alias (a_i) modulo N. Ceci permet de vérifier la donnée d'habilitation sans la connaître.

FIG.1



EP 0 294 248 A1

Description

Dispositif et procédé d'habilitation informatique ou télématique.

L'invention concerne l'habilitation, en matière informatique ou télématique.

Elle trouve une application particulière, non limitative, dans ce qu'on appelle la "monétique", c'est-à-dire la réalisation quasi-automatique de transactions monétaires, commerciales ou financières.

L'exemple le plus simple d'habilitation consiste en la présentation par un usager d'une information ou donnée d'habilitation, telle qu'un code confidentiel, qu'il est en principe seul à connaître. La machine en face de laquelle il se trouve, ou "terminal", est équipée pour déterminer si le code confidentiel présenté est acceptable pour l'habilitation de l'usager à une action déterminée, telle que l'accès à des informations, ou la conclusion d'une transaction. Le contrôle de la validité d'un code confidentiel s'effectue actuellement selon des critères choisis, tenant compte d'autres informations, non secrètes, servant à repérer l'usager, comme celles figurant sur un relevé d'identité bancaire.

Dès lors que l'usager doit présenter son code confidentiel, celui-ci est nécessairement introduit dans le terminal. Il existe donc un risque qu'il soit intercepté. L'intercep teur est alors en mesure de "simuler" l'usager légitime du code confidentiel.

Dans les applications actuelles, le risque d'interception est rendu très faible, par le fait que la circulation du code confidentiel dans le terminal est confinée à un espace contrôlé, et/ou qu'il fait l'objet d'un chiffrement, en cas de transmission à distance.

La présente invention a pour but d'améliorer encore la sécurité, en permettant d'établir une habilitation sans que le vérificateur n'ait à connaître la ou les données d'habilitation elles-mêmes (code confidentiel par exemple).

Pour alléger la suite de la présente description, on appelle "entier" un nombre entier, ou tout équivalent d'un nombre entier qui serait exprimé en format fixe, indépendamment du fait qu'il contient ou non une virgule. Un entier peut également être la transposition en code binaire, de format fixe, de toute information alphanumérique.

Les expressions "tirage au sort" et "aléatoire", qualifiant un "entier", visent la possibilité d'obtenir matériellement, dans un circuit, un nombre entier aléatoire ou pratiquement aléatoire, dans la limite du format choisi pour les entiers. Un tel tirage au sort peut, par exemple, être réalisé à l'aide d'un générateur de séquences pseudo-aléatoires.

Le dispositif d'habilitation informatique ou télématique de l'invention est du type dans lequel un poste demandeur d'habilitation détient au moins une donnée de repérage et au moins une donnée d'habilitation, en principe secrète, dont il doit justifier auprès d'un poste vérificateur, pour contrôle de validité selon des critères choisis.

L'homme de l'art comprendra que la donnée de repérage peut être une donnée numérique classique physiquement disponible dans le poste demandeur d'habilitation, ou bien résulter simplement de caractéristiques physiques de celui-ci, comme une liaison particulière dont il dispose à l'égard du poste vérificateur.

Selon une première caractéristique de l'invention, le poste demandeur comprend, dans un circuit protégé :

- des moyens de mémoire de ladite donnée d'habilitation sous la forme d'un entier d'habilitation dit "alias",
- des moyens de tirage au sort, propres à définir des entiers aléatoires auxiliaires,
- de premiers moyens de calcul propres à effectuer une première opération, non réversible, à un seul opérande entier,
- de seconds moyens de calcul propres à effectuer une seconde opération à deux opérandes entiers, la première opération étant conservative à l'égard de cette seconde opération,

et, en dehors du circuit protégé :

- des moyens d'interfaces propres à fournir sélectivement la donnée de repérage, une première quantité représentant le transformé d'un entier aléatoire auxiliaire par la première opération, ainsi qu'une seconde quantité représentant soit le transformé par la seconde opération de ce même entier aléatoire et de l'alias, soit cet entier aléatoire lui-même.

Ceci permet de vérifier la donnée d'habilitation sans la connaître, et de vérifier le caractère aléatoire des entiers auxiliaires.

Avantageusement, la première opération est une élévation à une puissance, en particulier la puissance 3, modulo N, N étant un nombre entier public prédéterminé possédant un large spectre de restes en tant que diviseur dans une division entière, ce que l'on appelle aussi un entier difficile ment factorisable. En particulier, N est un nombre premier ou un produit de deux nombres premiers.

La seconde opération peut être une multiplication modulo N.

Selon une autre caractéristique, non impérativement nécessaire, de l'invention, le poste vérificateur comprend :

- une mémoire propre à contenir, en correspondance du repérage de chaque poste demandeur, au moins une quantité de référence représentant le transformé de l'alias par la première opération,
- des moyens de calcul propres à effectuer la première et la seconde opération,
- des moyens d'interface propres à recevoir d'un poste demandeur la donnée de repérage et la première quantité, à lui transmettre un signal d'indice susceptible de prendre au moins deux états différents, ainsi qu'à recevoir ensuite, selon l'indice, la seconde quantité ou l'entier aléatoire,
- des moyens d'interrogation susceptibles d'au moins deux états différents commandant ceux du signal d'indice, et réagissant à la réception d'une donnée de repérage et d'une première quantité en prenant au choix un de ces deux états, pour demander la seconde quantité associée au même entier aléatoire ou l'autre de ces deux états pour

demander l'entier aléatoire lui-même, et

- des moyens logiques de décision d'habilitation en fonction, suivant l'état choisi, soit de la concordance du transformé de la seconde quantité par la première opération et du transformé de la première quantité et de la quantité de référence par la seconde opération, soit de la concordance de la première quantité avec le transformé de l'entier aléatoire par la première opération.

Cependant, l'invention acquiert une puissance bien supérieure lorsque le poste demandeur possède, en mémoire secrète, un nombre prédéterminé d'alias, formant une suite rangée. Le poste vérificateur contient alors en mémoire une partie au moins de la suite ordonnée correspondante de quantités de référence. Ses moyens d'interrogation possèdent un nombre d'états différents au plus égal au nombre d'alias, augmenté de 1.

Le poste vérificateur peut ainsi demander, pour chaque première quantité reçue en correspondance d'un entier aléatoire, soit l'entier aléatoire d'origine, soit toute combinaison de celui-ci par la seconde opération avec l'un quelconque des alias.

Très avantageusement, le poste vérificateur comporte en outre des moyens propres à vérifier le caractère aléatoire des entiers auxiliaires, à partir d'une mémorisation de ceux-ci sur un intervalle de temps suffisant.

Dans un mode de réalisation de l'invention, le poste demandeur est situé à distance du poste vérificateur, et relié à celui-ci par modems. Il émet d'abord une série de premières quantités relatives à des entiers aléatoires différents (ou plus exactement résultant de tirages différents, dont il peut arriver qu'ils donnent le même résultat). Le poste vérificateur établit alors une "interrogation" paramétrée, non connue à l'avance du demandeur. Ensuite, la réponse du demandeur délivrera l'ensemble des résultats comprenant, en correspondance de chaque première quantité, soit l'entier aléatoire, soit la seconde quantité, selon le paramètre d'interrogation reçu du poste vérificateur.

Dans un autre mode de réalisation de l'invention, le poste demandeur est situé localement au même point que le poste vérificateur auquel il est directement relié. Le poste demandeur peut alors établir ses entiers aléatoires un par un. Le dialogue d'habilitation consiste en une suite de questions portant chacune sur une première quantité relative à un entier aléatoire déterminé (en cours pour le poste demandeur), et ensuite soit sur cet entier aléatoire lui-même, soit sur la seconde quantité qui correspond à ce même entier aléatoire et à un entier d'habilitation désigné.

Dans la mesure où le caractère non réversible de la première opération est suffisamment assuré, on peut aussi concevoir que le poste demandeur transmette le transformé, par cette première opération, de l'un au moins de ses alias.

Ceci est d'ailleurs une manière d'assurer le repérage du poste demandeur, pour le poste vérificateur.

L'invention offre aussi un procédé d'habilitation informatique ou télématique entre au moins un poste demandeur et au moins un poste vérificateur. Ce procédé comporte les étapes suivantes :

a) mémoriser préalablement au moins un entier d'habilitation ou "alias" dans le poste demandeur,

b) équiper le poste demandeur de moyens propres au tirage au sort d'entiers auxiliaires aléatoires,

c) équiper le poste demandeur et le poste vérificateur de moyens de calcul propres à effectuer une première opération, non réversible, à un seul opérande entier, et une seconde opération à deux opérandes entiers, la première opération étant conservative à l'égard de la seconde,

d) à un moment quelconque, mémoriser dans le poste vérificateur le transformé du ou des alias par la première opération,

e) lors d'une demande d'habilitation qui est supposée provenir du poste demandeur :

e1) recevoir au poste vérificateur le transformé par la première opération d'au moins un entier aléatoire déterminé,

e2) émettre du poste vérificateur un signal d'indice possédant au moins deux états différents,

e3) recevoir au poste vérificateur une quantité qui, selon l'état du signal d'indice, est supposée représenter soit l'entier auxiliaire aléatoire, soit le transformé de cet entier auxiliaire aléatoire et de l'alias par la seconde opération,

e4) décider de l'habilitation en fonction de l'exactitude de la quantité reçue.

Une manière particulière de mettre en oeuvre ce procédé consiste à répéter les étapes e1) à e3), à la volonté du poste vérificateur, en faisant changer à chaque fois l'entier auxiliaire aléatoire et/ou l'alias concerné. Le poste vérificateur peut ainsi poser autant de questions qu'il le veut, jusqu'à ce qu'il ait obtenu, avec un taux de vraisemblance suffisant, la preuve de l'habilitation du poste demandeur.

Une autre mise en oeuvre du procédé consiste en ce que l'étape e1) s'effectue pour une série d'entiers aléatoires en nombres choisis; l'étape e2) porte alors sur un signal d'indice complété d'une désignation d'alias, en correspondance de chaque entier auxiliaire aléatoire; l'étape e3) porte le cas échéant sur l'alias désigné pour chaque entier auxiliaire.

Bien entendu, on pourra concevoir aisément d'autres variantes du dispositif et du procédé qui viennent d'être exposés.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 est un schéma de principe d'un dispositif permettant la mise en oeuvre de l'invention; et

- la figure 2 est un organigramme d'un exemple de mise en oeuvre du procédé selon l'invention, appliqué à une authentification unidirectionnelle.

Les dessins annexés comportent, pour l'essentiel, des éléments de caractère certain. En conséquence, ils pourront non seulement servir à mieux

faire comprendre la description détaillée, mais aussi contribuer à la définition de l'invention, le cas échéant.

Par ailleurs, il est clair que la description détaillée ci-après concerne un exemple d'application de l'invention, donné à titre non limitatif.

Sur la figure 1, le poste demandeur d'habilitation DH comporte un circuit secret CDH, une interface IDH, également désignée par la référence 20, et un modem MDH également désigné par la référence 29.

Le caractère secret du circuit CDH est matérialisé sur le dessin par le fait que celui-ci est entouré d'un cadre en trait doublé.

Le poste vérificateur VH comporte un circuit CVH, qui n'a pas impérativement besoin d'être secret, mais peut avantageusement l'être. Il s'y ajoute une interface IVH également désignée par la référence 40, et un modem MVH désigné aussi par la référence 49.

L'homme de l'art comprendra que la liaison par modem s'entend si les postes DH et VH sont distants. Lorsqu'ils sont rapprochés, on peut prévoir une liaison directe 50 entre les deux interfaces 20 et 40.

Le circuit secret CDH comporte une mémoire 10 servant à contenir les alias a_i qui sont les entiers d'habilitation.

Ces entiers sont exprimés dans un format fixe de longueur L.

Le circuit CDH comporte également un générateur 13 d'entiers aléatoires r_i, qui sont en principe de même longueur L que les alias.

Le circuit CDH comporte encore un premier organe de calcul 11 capable d'effectuer une élévation au cube modulo N d'un entier de longueur L.

L'élévation au cube de nombres entiers est une opération connue de l'homme de l'art. Etant réalisée modulo N, elle est simplifiée, puisqu'après chaque multiplication il est possible d'effectuer une division par N du résultat et de poursuivre les calculs en utilisant le reste. La taille des registres de calcul s'en trouve réduite d'autant.

Comme précédemment indiqué, N est un nombre premier ou un produit de deux nombres premiers. On pourra par exemple prendre N égal au nombre premier immédiatement supérieur à une puissance entière de 2, comme 65537. Cela peut aussi simplifier les calculs.

Le circuit 11 réalise la première opération à un opérande. Par exemple il fournit le reste de la division de la puissance cubique de son entrée par le nombre N. Dès lors que le nombre N possède un large spectre de restes, couvrant une large partie des valeurs de restes possibles de 0 à N, et de préférence toutes ou presque toutes ces valeurs, il apparaît que l'opération de calcul effectuée par l'organe 11 est non réversible, et qu'il est d'autant plus difficile de trouver le nombre entier d'entrée appliqué à l'organe 11.

Un second organe de calcul 12 réalise une opération à deux opérandes, comme par exemple une multiplication modulo N. Cette opération est dénotée par l'opérateur "." sur la figure 1, ou bien d'un carré marqué d'une croix de Saint André sur la figure 2.

Il est nécessaire que la première opération soit conservative à l'égard de la seconde. Cela signifie la chose suivante : soient x et y deux entiers.Le cube modulo N du produit de ces deux entiers par la seconde opération (une multiplication modulo N) doit être égal au produit des cubes modulo N de x et de y.

Il existe d'autres couples d'opérations entières susceptibles de satisfaire cette condition.

Le circuit secret CDH contient encore une logique de commande 15 qui contrôle la mémoire 10, le générateur d'entiers aléatoires 13, les deux organes de calcul 11 et 12, ainsi que les sorties d'informations du circuit secret CDH, lesquelles ne peuvent porter que sur des sorties des organes de calcul 11 et 12 ou sur la sortie du générateur d'entiers aléatoires, à l'exclusion bien entendu de la sortie de la mémoire d'alias 10. Le cas échéant, la logique de commande 15 peut également fournir à l'interface 20 les données repérant ou identifiant le poste demandeur DH. (le mot "identifiant" est évité dans la présente description, car les données d'habilitation peuvent très bien comprendre les données d'identification; on parle simplement de "repérage" lorsqu'il s'agit de désigner le poste demandeur concerné.)

L'échange de données qui est ainsi possible à travers l'interface demandeur 20 transite directement ou par modem vers le poste vérificateur VH.

Le circuit CVH de celui-ci comprend une mémoire 30 susceptible de contenir les transformées A_i par la première opération des alias a_i de chacun des postes demandeurs qui peuvent solliciter une habilitation. Incidemment, on observera que lorsqu'un entier de base est désigné par une minuscule, son transformé par la première opération est désigné en principe par la majuscule correspondante.

Le circuit CVH comprend également un organe de calcul 31 capable d'effectuer les première et seconde opérations. Il comprend aussi une logique de commande et de décision 35, dans laquelle on pourra distinguer des moyens d'interrogation proprement dits et des moyens de décision, en plus des fonctions de commande générales des mémoires et de l'organe de calcul ainsi que des entrées/sorties d'informations du circuit CVH.

Ce circuit CVH comporte encore une mémoire tampon 37 capable de recevoir les premières quantités R_i qui vont venir d'un poste demandeur. Ces premières quantités R_i sont des transformées, supposées établies dans le poste demandeur, d'un nombre entier aléatoire de base R_i.

Mais il est également à craindre qu'un intrus ait intercepté la valeur R_i lors de sa circulation entre les deux postes. Ceci ne lui donne pas, pour autant, accès à l'entier aléatoire de base r_i.

Pour engendrer l'interrogation, il est avantageux de prévoir un organe spécialisé 32. Il procède par tirage aléatoire, ou encore selon un algorithme spécifique inconnu des demandeurs, et imprévisible de ceux-ci.

Une autre mémoire tampon 38 va servir à stocker d'autres informations qui peuvent être soit une seconde quantité p_i, soit le transformé de celle-ci par la première opération, noté exceptionnellement

WD_i (plutot que P_i).

Dans le cas d'une identification unidirectionnelle, le circuit CVH n'est pas nécessairement un circuit secret comme le circuit CDH. En pratique, pour certains modes de réalisation de l'invention au moins, on aura cependant intérêt à ce que le circuit CVH soit un circuit secret, compte tenu de son aptitude à accumuler un nombre assez important d'informations résultant de la mise en oeuvre de l'invention. La connaissance de cet ensemble d'informations pourrait en effet diminuer la sécurité de l'invention.

On reviendra brièvement sur les circuits CDH. En regard de la logique de commande, il apparaît un cadre 16 en trait tireté, dans lequel les connexions issues de la mémoire 10 et du générateur 13 vers les organes de calcul ou vers l'extérieur sont chacune marquées d'un cercle. Ces cercles schématisent un interrupteur placé sous le controle de la logique de commande 15. On notera également une liaison en trait tireté entre la mémoire 10 et l'organe de calcul 11. Cette liaison peut servir à transmettre des valeurs A_i, pour les applications où celles-ci ne seraient pas toutes inscrites a priori dans la mémoire 30 du ou des postes vérificateurs.

La figure 2 permettra maintenant de mieux comprendre l'invention, sur un exemple élémentaire de mise en oeuvre du procédé. L'indice i utilisé sur la figure 2 montre que l'interrogation ou question élémentaire dont il s'agit a vocation à être répétée.

L'étape 101 consiste en un tirage au sort, dans le circuit 13, d'un entier auxiliaire aléatoire r_i.

L'étape 102 consiste en un actionnement de l'organe de calcul 11 par la logique de commande 15, ce qui fournit le transformé R_i de l'entier aléatoire de base. L'étape 103 consiste en la transmission, sous le contrôle de la logique de commande 15, et à travers l'interface 20, de la grandeur R_i vers le poste vérificateur VH. Il est supposé que, vu du côté de ce poste vérificateur, le poste demandeur DH est "repéré". Ceci peut se faire de toute manière adéquate, notamment de celles évoquées plus haut.

A l'étape 204, le poste VH reçoit par son interface 40 la grandeur R_i. Sous le contrôle de la logique 35, cette grandeur est appliquée à l'organe de calcul 31, pour effectuer la seconde opération de calcul, comme matérialisé en l'étape 206, en correspondance de l'une des quantités de référence A_i disponibles dans la mémoire 205.

En même temps, la logique de commande 35 actionne la mémoire 37, comme indiqué en l'étape 207, pour qu'elle stocke la grandeur R_i et, en principe, la grandeur R_i-A_i.

L'homme de l'art comprendra cependant que, pour certains modes de réalisation de l'invention au moins, la réalisation des étapes 205, 206 et de la mise en mémoire $R_i.A_i$ peut être différée jusqu'à ce qu'on connaisse la valeur de s_i.

Ce qui vient d'être décrit concerne la première partie d'une "question"; cette première partie est consécutive à l'émis-sion d'au moins un entier aléatoire par le poste demandeur, d'où il résulte certaines actions dans le poste vérificateur VH.

Après cela, l'étape 211 consiste en la définition d'un signal d'indice S_i.

Dans une version tout à fait élémentaire du procédé selon l'invention, ce signal d'indice ne prend que deux valeurs, par exemple 0 et 1. Le signal en question est transmis au poste demandeur DH. Si sa valeur est 0, des aiguillages, schématisés ici par des contacteurs, sont placés tous les deux dans leur position de gauche. S_i la valeur de S_i est 1, ils sont au contraire placés dans leur position de droite.

Cependant, il est plus avantageux que le signal d'indice s_i puisse prendre d'autres valeurs. Celles-ci servent alors à désigner l'un des alias. Cette désignation vient donc d'un côté, dans le poste vérificateur VH, définir la sélection dans la mémoire 205 de celle des quantités de référence A_i qui va être appliquée à l'opérateur 206. Dans le poste demandeur DH, cette désignation sert à définir celui des alias a_i contenus dans la mémoire secrète 10 qui va, à l'étape 112, être appliqué pour la réalisation de l'étape 113 qui est une mise en oeuvre du second organe de calcul 12 par la logique de commande 15.

La logique de commande 15 peut alors mémoriser à l'étape 114 d'une part l'entier aléatoire auxiliaire r_1 (supposé toujours disponible en sortie du générateur 13), et d'autre part le produit $r_i.a_i$ issu de l'étape 113.

On observe maintenant que, quelle que soit la position des commutateurs 115 et 215, et la valeur d'indice définie par le signal s_i, on dispose en sortie des commutateurs 115 et 215, respectivement, d'une quantité de base notée p_i, du coté du poste demandeur DH, et, du côté du poste vérificateur VH, d'une quantité WV_i qui est supposée être le transformé de cette quantité de base par la première opération.

La quantité de base p_i est soit l'entier aléatoire r_i luimême, soit une seconde quantité représentant le produit de l'entier aléatoire r_i et de l'alias a_i par la seconde opération.

L'étape 117 consiste en la transmission de la quantité p_i du poste demandeur DH vers le poste vérificateur VH où elle est reçue comme matérialisé à l'étape 218 à travers l'interface 40.

La logique de commande 35 applique ce signal p_i à l'organe de calcul 31, où il subit la première opération comme indiqué en 219, ce qui fournit le transformé WD_i de p_i par cette première opération.

La logique de commande 35 intervient alors comme indiqué à l'étape 220 pour prendre une décision ou une décision partielle, en fonction de la comparaison de WD_i reçu et de WV_i calculé localement.

Le mécanisme de prise de décision lui-même peut faire l'objet de très nombreuses variantes, dès lors qu'on disposera d'un nombre suffisamment important de comparaisons élémentaires effectuées à l'étape 220.

Cela étant, on peut considérer schématiquement que toute comparaison invalide se traduira par la non habilitation du poste demandeur. Mais, pour un très grand nombre de comparaisons, on peut admettre que quelques-unes d'entre elles soient erronées, sous certaines conditions.

Comme déjà indiqué, ce qui vient d'être décrit en référence à la figure 2 est une mise en oeuvre "élémentaire" du procédé selon l'invention. Cette

mise en oeuvre élémentaire peut être résumée comme suit :

En réponse à chaque tirage au sort d'un entier aléatoire r_i, et à la transmission de son transformé R_i, le poste vérificateur peut demander soit ce nombre aléatoire r_i luimême, soit le produit par la seconde opération de l'entier aléatoire et de l'un quelconque, désigné par le signal s_i, des alias a_i.

En posant à volonté le nombre de questions de ce type qui lui convient, le poste vérificateur peut disposer d'autant de résultats de comparaison 220 qu'il veut.

A priori, on admettra que toute comparaison invalide suffit à disqualifier un poste demandeur. Le nombre de questions posées pourra alors être fixé en fonction d'un taux de sécurité à respecter qui peut être soit prédéterminé, soit ajusté à volonté cas par cas par le poste vérificateur.

Dans ce qui vient d'être décrit, différentes questions sont posées séquentiellement. Il est bien entendu possible, et plus intéressant dans le cas d'une transmission par modem, de les poser en parallèle.

Dans ces conditions, ce n'est pas un tirage au sort mais une série de tirages au sort que va transmettre initialement le poste demandeur DH au poste vérificateur VH.

Le nombre de tirages au sort n'est pas limité au nombre d'alias existants, car :

- d'une part, certains nombres tirés au sort ne serviront pas à la confirmation d'un alias, mais seront simplement vérifiés eux-mêmes;
- d'autre part il peut être souhaitable de vérifier un ou plusieurs alias en considérant leurs produits par plusieurs entiers aléatoires.

Un signal d'indice s_i est alors transmis pour chaque entier aléatoire tiré au sort.

En conséquence, on disposera d'autant de secondes quantités P_i que de premières quantités R_i.

Finalement, on dispose d'un nombre de comparaisons 220 égal au nombre d'entiers aléatoires r_i initialement défini.

Dans ce dernier mode de réalisation, on peut se contenter de poser une seule question multiple. Mais, si une sécurité supérieure est désirée, le poste vérificateur VH peut interroger le poste demandeur DH pour une nouvelle série de tirages au sort, et ainsi de suite.

Dans un exemple de réalisation de l'invention, le nombre premier N est égal à 65537.

Chaque entité (poste demandeur) se donne K alias différents, avec K égal à 7 ou 15 par exemple, ces alias étant numérotés de 1 à K.

L'étape 101 consiste à tirer m nombres au hasard r_i, dont il envoie les transformés R_i par la première opération (premières quantités). Après avoir effectué les opérations déjà décrites, le poste vérificateur va renvoyer m valeurs du signal d'indice s_i, pouvant aller de 0 à K, avec la contrainte que ces valeurs ne sont pas toutes nulles, de façon qu'au moins un alias soit vérifié. Ceci détermine la spécificité de l'interrogation faite par le poste vérificateur, et garantit ainsi la personnalisation de la réponse.

Le poste demandeur devra renvoyer les N produits de la forme :

$p_i = r_i.a_j$ avec $j = s_i$ et, par définition, $a_0 = 1$. En effet, à la valeur 0 du signal d'indice s_i, le poste demandeur répond en envoyant purement et simplement son nombre entier aléatoire r_i.

La vérification peut s'effectuer de la même manière, c'est-à-dire en faisant systématiquement des produits de la forme:

$WV_i = R_i.A_j$, avec par définition $A_0 = 1$.

Cette remarque ouvre la voie à une réalisation particulièrement simple, permettant d'éviter les commutations illustrées en 115 et 215, puisque les cas où l'on considère seulement le nombre aléatoire peuvent très bien être considérés comme un produit de celui-ci par l'unité (plus exactement par l'élément neutre de la seconde opération).

Les valeurs K et m sont déterminées de façon que la probabilité $2^{-(k+1)m}$ pour que la même séquence soit redemandée à un poste demandeur identique soit très faible.

En pratique, on pourrait imaginer les couples suivants:

$K = 1$, $m = 10$
$K = 18$, $m = 1$
$K = 7$, $m = 3$

En prenant d'ores et déjà des valeurs $K = 7$ et $m = 3$ ou $K = 3$ et $m = 6$, la probabilité sus-mentionnée est déjà au moins égale à 2^{-24}.

Dans les applications courantes, on peut se contenter de $K = 3$ et $m = 4$, ce qui donne encore une probabilité inférieure à deux cents millièmes, où $K = 1$ et $m = 8$, ce qui donne le même résultat.

On donnera maintenant un exemple particulier d'application de l'invention.

EXEMPLE

Données de base :

$N = 2^{16} + 1 = 65537$, nombre premier
$K = 3$, $m = 4$

Identités secrètes :

$a_1 = 11111$
$a_2 = 22222$
$a_3 = 33333$

Quantités de référence A_j, obtenues par élévation au cube modulo N.

$A_1 = 16119$
$A_2 = 63415$
$A_3 = 41991$

Tirage au sort des nombres aléatoires (étape 101).

$r_1 = 12345$
$r_2 = 34567$
$r_3 = 56789$
$r_4 = 78901$

Calcul et transmission des premières quantités R_i (étapes 102, 103).

$R_1 = 23289$
$R_2 = 64918$
$R_3 = 12729$
$R_4 = 12602$

Détermination des quatre valeurs du signal d'indice s_i, choisi par tirage au sort entre 0 et 3 (étape 211).

$s_1 = 2$
$s_2 = 0$
$s_3 = 2$
$s_4 = 3$

Détermination des produits p_i, par multiplication modulo N (étapes 113, 114, 115).

$p_1 = 58245$

$p_2 = r_2 = 34567$

$p_3 = 50223$

$p_4 = 07223$

Le simple examen des valeurs qui viennent d'être données pour cet exemple montre qu'aucune des informations transmises n'a de rapport avec les alias secrets a_1 à a_3.

Calcul des produits WV_i (étapes 206, 207 et 215).

$WV_1 = 61177$

$WV_2 = 64918$

$WV_3 = 55843$

$WV_4 = 24844$

Transformation par la première opération des valeurs p_i (étape 219).

$WD_1 = 61177$

$WD_2 = 64918$

$WD_3 = 55843$

$WD_4 = 24844$

Vérification d'identité (étape 220) par la correspondance entre les WV_i et les WD_i.

Comme déjà indiqué, l'invention est susceptible de nombreuses variantes, notamment celles incluses dans le cadre des revendications ci-après.

Pour certaines applications, on peut par exemple envisager que l'étape 219 de la figure 2 soit mise en oeuvre dans le poste demandeur DH. Ceci supprime la nécessité d'effectuer la première opération dans les postes vérificateurs. En contrepartie, il devient moins facile de vérifier le caractère aléatoire des tirages au sort effectués en 101 dans le poste demandeur.

Par ailleurs, il est bien entendu possible d'intercaler, dans la mise en oeuvre du procédé selon l'invention, des interrogations portant sur le transformé A_i des alias a_i par la première opération.

Enfin, les exemples décrits concernent une authentification unidirectionnelle. L'extension à une authentification mutuelle s'en déduit immédiatement, en prévoyant naturellement des circuits secrets de chaque côté.

A côté de cela, la longeur L du format des nombres entiers peut aller, suivant les applications, de 4 octets (utilisation pour habilitation individuelle, par code confidentiel) à des valeurs beaucoup plus élevées (transactions électroniques inter-bancaires).

De même, pour augmenter la sécurité, la première opération peut être une élévation à une puissance entière plus grande que trois.

Sur un autre plan, il est clair qu'on pourra chercher à restreindre autant que possible la connaissance des transformés A_i des alias a_i. Ainsi, chaque poste vérificateur peut ne disposer que d'une partie de ces transformés.

Revendications

1. Dispositif d'habilitation informatique ou télématique.

dans lequel un poste demandeur d'habilitation (DH) détient au moins une donnée de repérage, et au moins une donnée d'habilitation, en principe secrète, dont il doit justifier auprès d'un poste vérificateur (VH), pour contrôle de validité selon des critères choisis,

caractérisé en ce que le poste demandeur (DH) comprend, dans un circuit protégé (CDM) :

- des moyens de mémoire (10) de ladite donnée d'habilitation sous la forme d'un entier d'habilitation dit "alias",
- des moyens de tirage au sort (12), propres à définir des entiers aléatoires auxiliaires,
- des premiers moyens de calcul (11) propres à effectuer une première opération, non réversible, à un seul opérande entier,
- de seconds moyens de calcul (12) propres à effectuer une seconde opération à deux opérandes entiers, la première opération étant conservative à l'égard de cette seconde opération,

et, en dehors du circuit protégé, des moyens d'interface (IDH) propres à fournir sélectivement la donnée de repérage, une première quantité représentant soit le transformé d'un entier aléatoire auxiliaire par la première opération, ainsi qu'une seconde quantité représentant le transformé par la seconde opération de ce même entier aléatoire et de l'alias, soit cet entier aléatoire lui-même, ce qui permet de vérifier la donnée d'habilitation sans la connaître, et de vérifier le caractère aléatoire des entiers auxiliaires.

2. Dispositif selon la revendication 1, caractérisé en ce que la première opération est une élévation à une puissance, en particulier la puissance trois, modulo N, N étant un nombre entier public prédéterminé possédant un large spectre de restes en tant que diviseur dans une division entière, en particulier un nombre premier ou un produit de deux nombres premiers, et

en ce que la seconde opération est une multiplication modulo N.

3. Dispositif selon l'une des revendications 1 et 2, caractérisé en ce que le poste vérificateur (VH) comprend :

- une mémoire (30) propre à contenir, en correspondance du repérage de chaque poste demandeur, au moins une quantité de référence (A_i) représentant le transformé de l'alias (a_i) par la première opération,
- des moyens de calcul (31) propres à effectuer la première et la seconde opération,
- des moyens d'interface (40) propres à recevoir d'un poste demandeur la donnée de repérage et la première quantité, à lui transmettre un signal d'indice susceptible de prendre au moins deux états différents, ainsi qu'à recevoir ensuite, selon l'indice, la seconde quantité ou l'entier aléatoire,
- des moyens d'interrogation (35) susceptibles d'au moins deux états différents commandant ceux du signal d'indice, et réagissant à la réception d'une donnée de repérage et d'une

première quantité en prenant au choix l'un de ces deux états, pour demander la seconde quantité associée au même entier aléatoire, ou l'autre de ces deux états pour demander l'entier aléatoire lui-même, et

- des moyens logiques (35) de décision d'habilitation en fonction, suivant l'état choisi, soit de la concordance du transformé de la première quantité et de la quantité de référence par la seconde opération, soit de la concordance de la première quantité avec le transformé de l'entier aléatoire par la première opération.

4. Dispositif selon la revendication 3, caractérisé en ce que le poste demandeur (DH) possède, en mémoire secrète (10), un nombre prédéterminé d'alias, formant une suite rangée, en ce que le poste vérificateur (VH) contient en mémoire (30) une partie au moins de la suite ordonnée correspondante de quantités de référence et en ce que ses moyens d'interrogation (35) possèdent un nombre d'états différents au plus égal au nombre d'alias, augmenté de 1.

5. Dispositif selon l'une des revendications 3 et 4, caractérisé en ce que le poste vérificateur (VH) comporte également des moyens (37, 38, 35) propres à vérifier le caractère aléatoire des entiers auxiliaires.

6. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que le poste demandeur (DH), distant du poste vérificateur (VH), est relié à celui-ci par modems (29, 49), en ce qu'il émet d'abord une série de premières quantités relatives à des entiers aléatoires différents, et ensuite, en correspondance de chaque première quantité, soit l'entier aléatoire, soit la seconde quantité.

7. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que le poste demandeur (DH), local, est directement relié au poste vérificateur (VH), et en ce qu'il répond à une suite de questions portant chacune d'abord sur une première quantité relative à un entier aléatoire déterminé, et ensuite soit sur cet entier aléatoire, soit sur la seconde quantité qui correspond à celui-ci et à un entier d'habilitation désigné.

8. Dispositif selon l'une des revendications 1 à 7, caractérisé en ce que le poste demandeur (DH) est également capable de transmettre le transformé, par la première opération, de l'un au moins de ses alias.

9. Procédé d'habilitation informatique ou télématique entre au moins un poste demandeur et au moins un poste vérificateur, caractérisé par les étapes suivantes :

a) mémoriser préalablement (10) au moins un entier d'habilitation ou "alias" dans le poste demandeur,

b) équiper le poste demandeur de moyens (13) propres au tirage au sort d'entiers auxiliaires aléatoires,

c) équiper le poste demandeur et le poste vérificateur de moyens de calcul (11, 12; 31) propres à effectuer une première opération, non réversible, à un seul opérande entier, et une seconde opération à deux opérandes entiers, la première opération étant conservatrice à l'égard de la seconde,

d) à un moment quelconque, mémoriser dans le poste vérificateur (30) le transformé du ou des alias par la première opération,

e) lors d'une demande d'habilitation qui est supposée provenir du poste demandeur :

e1) recevoir au poste vérificateur (VH) le transformé par la première opération, d'au moins un entier aléatoire déterminé,

e2) émettre du poste vérificateur (VH) un signal d'indice possédant au moins deux états différents,

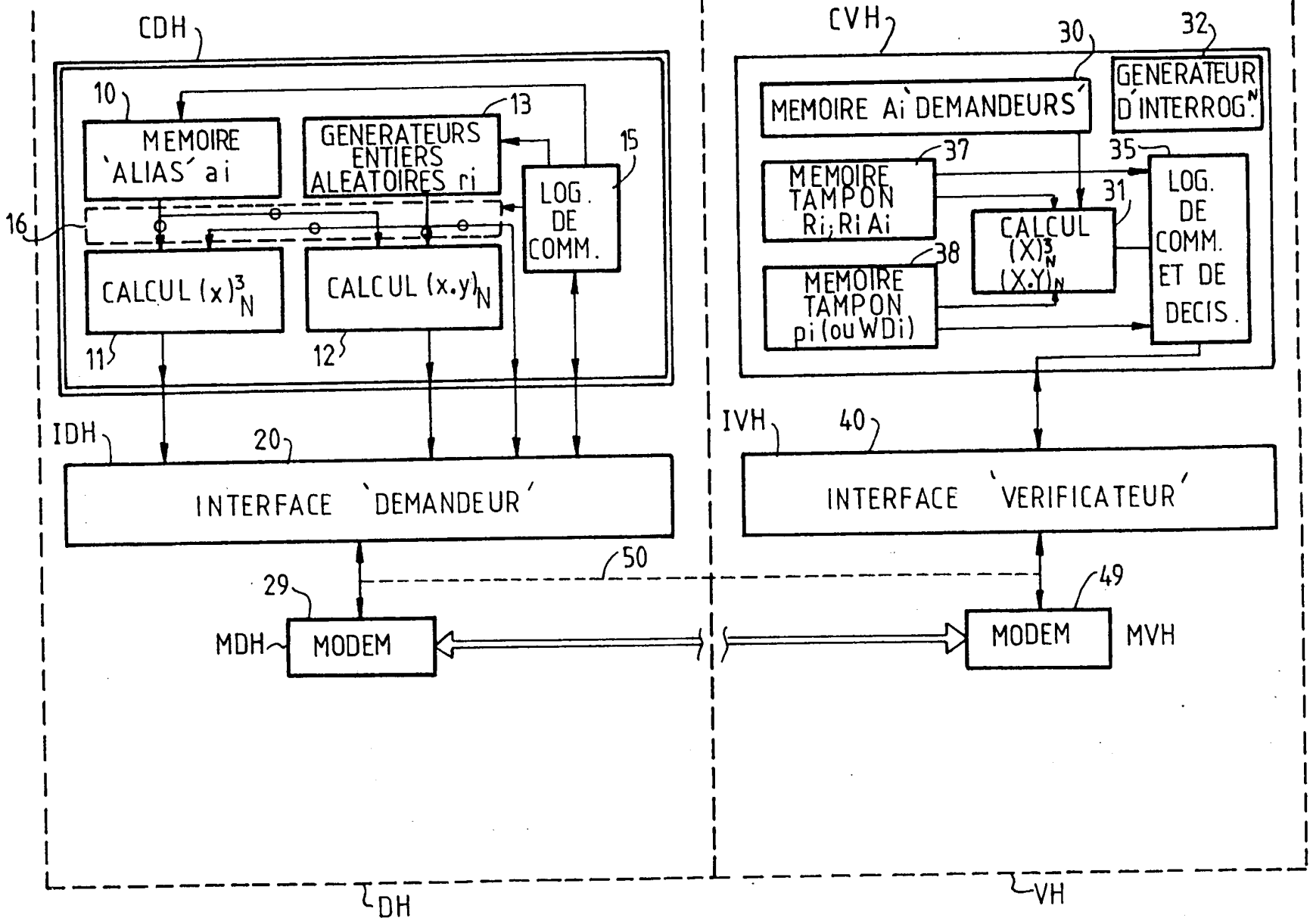
e3) recevoir au poste vérificateur (VH) une quantité qui, selon l'état du signal d'indice, est supposée représenter soit l'entier auxiliaire aléatoire, soit le transformé de cet entier auxiliaire aléatoire et de l'alias par la seconde opération,

e4) décider de l'habilitation en fonction de l'exactitude de la quantité reçue.

10. Procédé selon la revendication 9, caractérisé en ce que les étapes e_1) à e_3) sont répétées à la volonté du poste vérificateur (VH), en faisant changer à chaque fois l'entier auxiliaire aléatoire et/ou l'alias concerné.

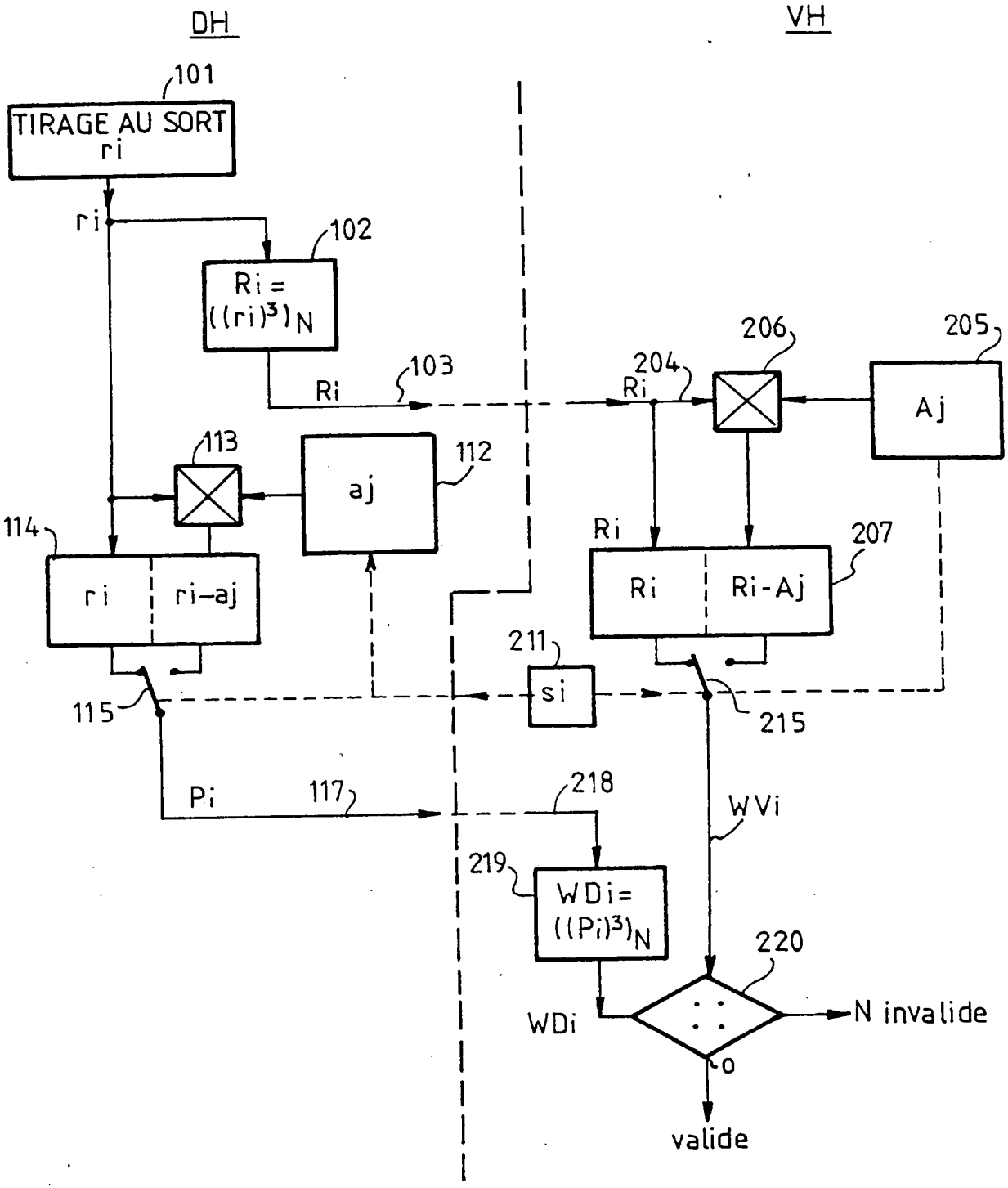
11. Procédé selon la revendication 9, caractérisé en ce que l'étape e1) s'effectue pour une série d'entiers aléatoires en nombre choisi,
l'étape e2) porte sur un signal d'indice complété d'une désignation d'alias, en correspondance de chaque entier auxiliaire aléatoire,
l'étape e3) porte, le cas échéant, sur l'alias désigné pour chaque entier auxiliaire.

FIG. 1



0294248

FIG. 2


DH
VH
101
TIRAGE AU SORT
ri
ri
102
Ri =
((ri)3)N
Ri
103
204
Ri
206
205
Aj
113
aj
112
114
ri
ri-aj
Ri
207
Ri
Ri-Aj
211
si
115
215
Pi
117
218
WVi
219
WDi=
((Pi)3)N
220
WDi
N invalide
0
valide

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 88 40 0930

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.4)
A	GB-A-2 020 513 (ATALLA TECHNOVATIONS) * Résumé; figures 1A-2B; page 2, lignes 15-9 *	1,3,4,6 ,7,9	G 07 F 7/10 H 04 L 9/00
A	EP-A-0 028 965 (CII-HB) * Résumé; figure 1 *	1,3,8,9	
A	EP-A-0 138 386 (TOSHIBA)		
A	EP-A-0 057 603 (W. WARD)		
A	FR-A-2 526 977 (CII-HB)		
A	GB-A-2 144 564 (PHILIPS)		
A	GB-A-2 019 060 (PITNEY BOWES)		

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)
G 07 F H 04 L

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	29-08-1988	DAVID J.Y.H.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)